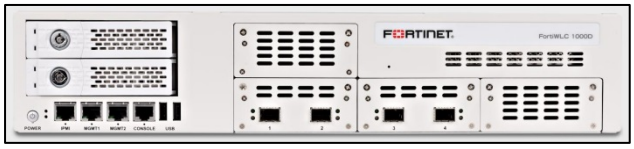
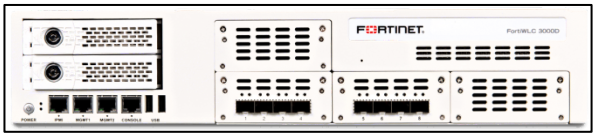
FORTINET
High Performance Network Security

FortiWLM

Release 8.3.0

FortiWLM 8.3.0 introduces support for new controllers, the FortiWLC-1000D and the FortiWLC-3000D.

Fortinet Wireless LAN Controllers

FortiWLC-1000D	FortiWLC-3000D
	

Additionally, FortiWLM 8.3.0 introduces new features and enhancements as listed under the new features section.

To ensure a secured Wi-Fi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Getting Started with Upgrade

This section describes procedures for upgrading your Services Appliance.

Important Update to Licensing

Starting with 8.3, FortiWLM will move to FortiCare Licensing.

All old Licenses will be overwritten and the correct values of AP's are maintained. FortiWLM will no longer count any features – but only maintain records of AP numbers. Features are recommended on maximum numbers according to hardware (new datasheet will contain these). The WLM-VM will come with 30-day trial licenses which will time out. When a WLM-VM is purchased a 50 AP Licenses key will be generated and sent to the customer.

RMA

In case of RMA of WLM/SA boxes with versions earlier than 8.3, restore the backup (if available) to restore existing flexnet licenses. Contact customer support if no backup is available for assistance to restore your existing licenses.

Upgrading SA2000 from FortiWLM 7.0-5 or 8.0 or 8.1

Before upgrading your legacy SA2000 appliance, execute the **`show nms`** command:

```
# sh nms
Server Parameters

Description : NM Server
Host Name : SCALE-2-WLM1000D
Uptime : 15d:23h:51m:45s
IP Address : 10.128.0.5
Netmask : 255.128.0.0
Default Gateway : 10.128.0.1
Public IP Address : 10.34.156.5
DHCP Server : 0.0.0.0
Software Version : 8.3-0GAbuild-1
```

```
Server Model : MVP2000
Manufacturing Serial # : FWM2KM1452008039
System Id : 1F77A44DC902
```

If the server model is listed as *MVP2000* and the serial number of your appliance starts with *FWM2KM****, contact the customer support for upgrade assistance.

Pre-requisites for upgrade

Upgrade service appliances (SA / FWLM) before you initiate controller (FortiWLC-SD) upgrade.

While upgrading a Services Appliance with over 100 controllers, the controllers return to *active* state sequentially, one at a time. It may take up to 10 minutes or more for all controllers to become active.

Supported FortiWLM Upgrades

The following upgrade path is recommended:

- 6.1-2-28 and/or 6.1-3-6 > 8.0-7-0
- 7.0-5-0 > 8.0-7-0
- 8.0-7-0 > 8.1-2-0
- 8.0-SR1-1 > 8.1-2-0
- 8.1-2-0 > 8.2-2-0
- 8.1-2-0, 8.1-3-0 > 8.3.0
- 8.2.2-0 > 8.3.0

Supported FortiWLC-SD Releases

Network Manager Version	Supports Controllers with these FortiWLC-SD Versions
8.3.0	• 7.0-9-1 • 7.0-10-MR • 8.0-6-0-MR • 8.1-2-0 • 8.1-3-2MR • 8.2-4-0 • 8.3.0

Supported Hardware and Software

Hardware / Software	Supported Versions/Models
FortiWLM/SAM - Access Points	• AP110 • AP320 • AP433 • OAP433 • AP832 • AP822 • AP122 • AP332 • AP1010 • AP1020 • OAP832e • FAP-U421EV • FAP-U423EV

Hardware / Software	Supported Versions/Models
SM	• PSM3X • AP832 • AP332 • AP1010 • AP1020
Controllers	• FortiWLC-50D • FortiWLC-200D • FortiWLC-500D • FortiWLC-1000D • FortiWLC-3000D • MC1550 • MC1550-VE • MC3200 • MC3200-VE • MC4200 • MC4200-VE • MC5000 • MC6000
Service Appliance	• FortiWLM-100D# • FortiWLM-1000D • SA250# • SA2000 • SA2000-VE • Hyper-V • KVM # Due to hardware limitations, High Availability is not supported in WLM100D and SA250 appliances
Cloud	• AWS EC2
Supported Browsers	• Internet Explorer 9 and later version *All the pages of the FortiWLM WebUI will load under normal browser settings. Compatibility View Settings are not supported*. • Mozilla Firefox 32.0 or higher • Google Chrome, version 34.0.1847.118 m • Apple Safari

Upgrade Recommendations

VPN Controllers

With the introduction of SHA2 support in FortiWLC-SD 8.1, any VPN controllers that are running SD version 8.0 or older and managed by Forti-WLM 8.1 or above will be disconnected from WLM after the upgrade. To fix this issue, apply the following patches for SHA2 support. Patch images are available for download from support portal.

1. Upgrade your Forti-WLM to 8.1 using the steps mentioned in the Upgrade Procedure section.
2. Apply the following patches on the managed VPN controllers:
    a. In 7.0 or older controllers, apply the following patches using the **`patch controller <version>`** command
        - meru-7.0-9-1-patch-Bug0353345-generic-rpm.tar

- meru-7.0-9-1-patch-Bug0363947-generic-rpm.tar

b. In 8.0 controller, apply the following patches using the **`patch install <version>`** command or upload the patch from WebUI (**Maintenance** > **File Management** > **Patches**).
   - meru-8.0-6-0-patch-Bug0353345-generic-rpm.tar
   - meru-8.0-6-0-patch-Bug0363947-generic-rpm.tar

3. After applying the patch, disable and enable VPN Client stat in the WebUI (**Configuration** > **Security** > **VPN Client**).

Application Visibility Policies

Application visibility policies in controllers running SD 8.0 that is managed by WLM 8.1 or later will be disabled. To continue using those policies, upgrade SD to 8.1 or later.

Upgrade Procedure

This procedure assumes that your Services Appliance is already installed on a network.

When upgrading from versions before FortiWLM 7.0, the DB is reset. It is therefore recommended that database backup should be taken before the upgrade and restored after the upgrade.

Upgrading via CLI

To upgrade a Services Appliance, perform the following steps:

1. Perform a complete Network Manager backup and copy the backup file to an external location. Use this if you run into a problem (Instructions for backing up the file can be found in the Maintenance chapter of the Network Manager User Guide.)
2. If you have SAM installed, disable all scheduled tests by performing the following steps:
   a. Select **Service Assurance**.
   b. From the left panel, select **Configure** > **Tests** > **Scheduled Tests**.
   c. Select the **Disable All** option and click **OK** continue.
3. Access the Services Appliance through SSH, using the administrative privilege.
4. If your appliance flash already contains three images, remove one of the older images using the `delete flash: <version number>` command.
5. Copy the file from the SCP server to your service appliance using the copy command:

   ```
   sa# copy scp://user:password@server/path/meru-nm-<releaseVersion>-SA250-rpm.tar<space>.
   ```

6. Confirm the successful transfer of the image by displaying the current flash images using the `sh flash` command:

   ```
   sa# sh flash
   6.0-7-0
   8.3.0
   ```

7. Upgrade the service appliance:

   ```
   sa# upgrade nms-server <Version>
   ```

This process installs new binaries and upgrades the stored data to the latest version. This process may take a few minutes, and at the end of the upgrade, the services appliance restarts. The time taken to upgrade depends on the size of the data available on the services appliance.

8. Type the following command to confirm this version of the software.

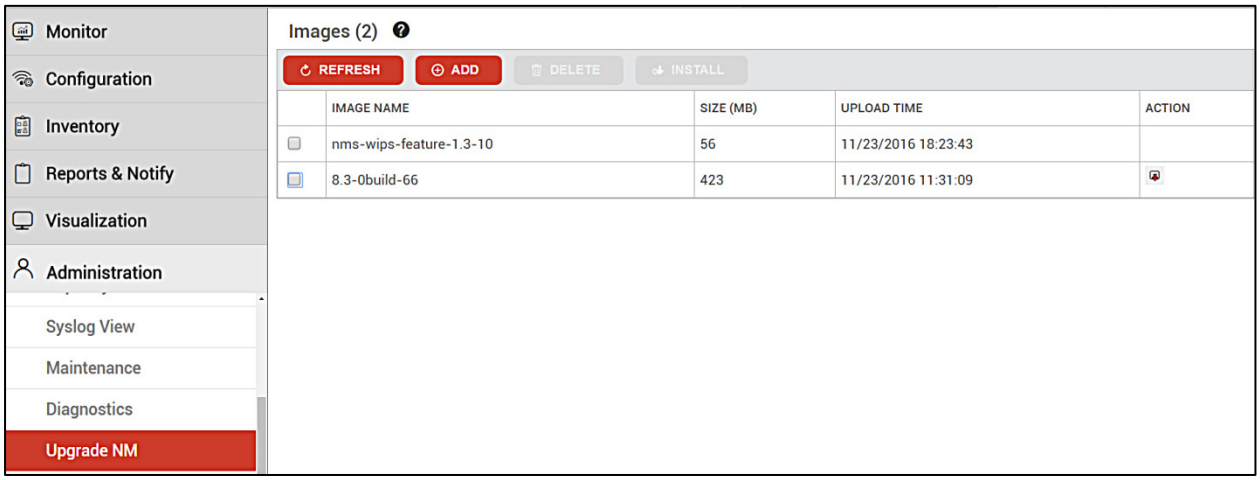
```
service appliance# sh nms
```

If the upgrade displays the "image integrity error," the service appliance image has been corrupted while uploading to Network Manager. Upload the new image again to the Network Manager service appliance and retry the upgrade. You can ignore the Security warning "Installing an unsigned upgrade package!" displayed by the upgrade command.

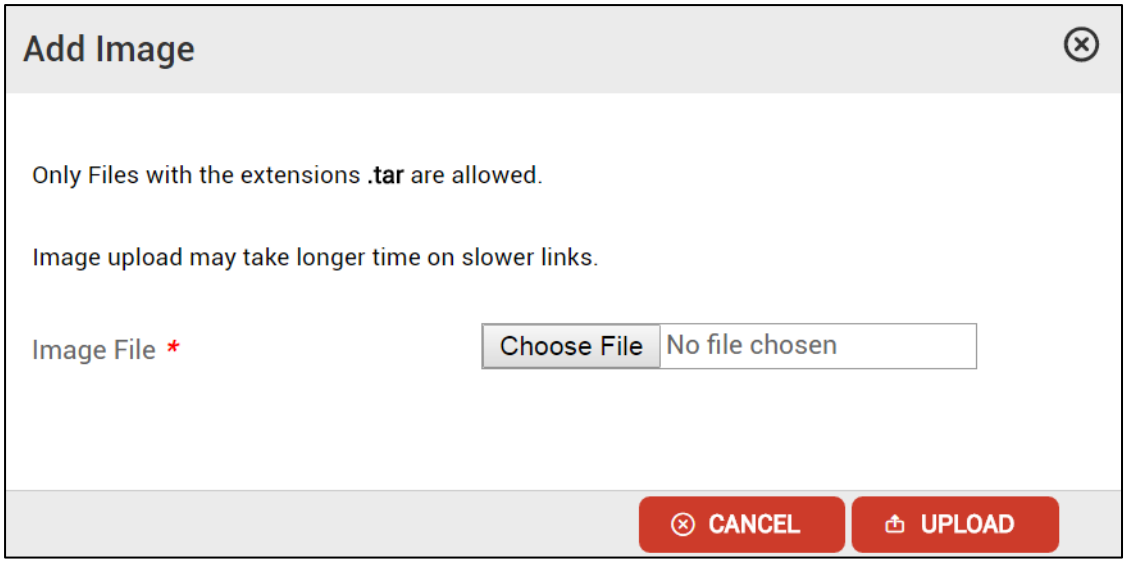
Upgrading via WebUI

The following procedure will guide you through the steps to upgrade your server from WebUI.

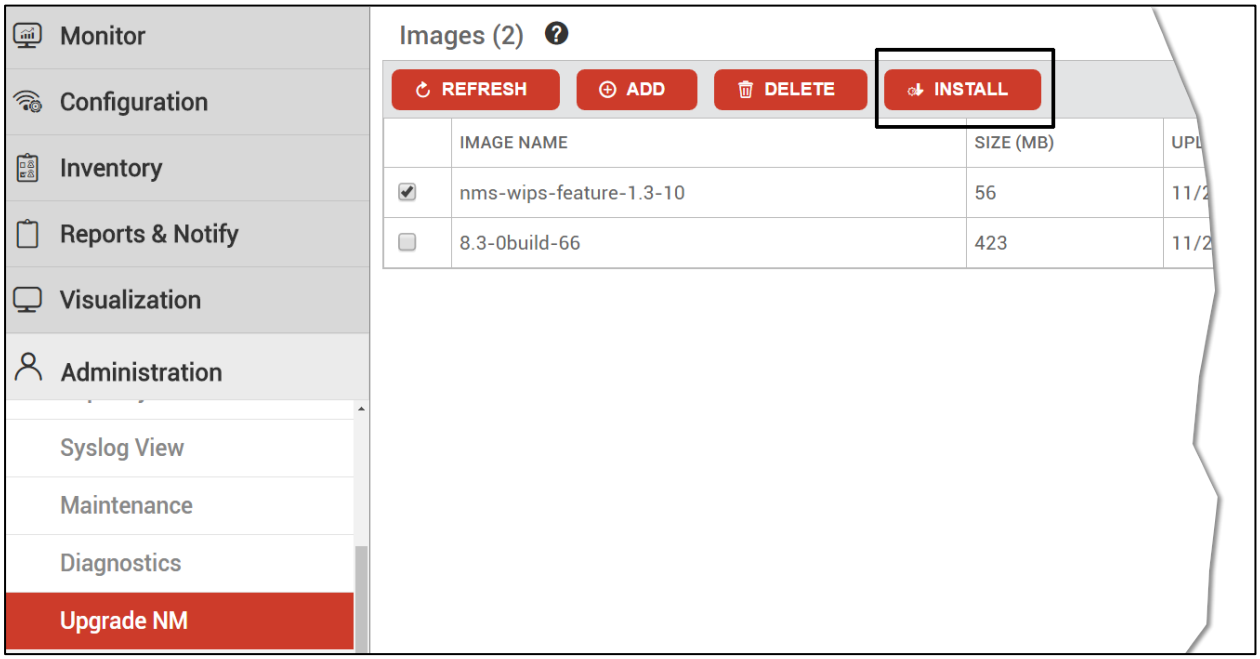
1. In the Network Manager WebUI, go to Administration > System Administration > Upgrade NM. By default, this page lists all the images copied to the server.



2. To upgrade your server to a different version than the ones listed, click **Add** to open the file selector window.



3. Select the image file from your computer or a network folder and click the **UPLOAD** button
4. After the upload is complete, select the version to install and click the **INSTALL** button to being the upgrade process.



During the upgrade process, do not click refresh or perform any operations on the server.

After the upgrade is complete, click Go the link to return to server operations.

- For a full upgrade, the server will restart after the upgrade process and return the page to server login prompt.
- For patch upgrade, the server will restart the process and return to the dashboard.

Post-Upgrade Tasks

The following are optional post-upgrade tasks:

1. If you have not configured for automatic transfer of backup to a remote server, then follow the instructions for configuration in the **Administration** > **Maintenance** page.
2. If required, upload the license.

Install the application images downloaded in the pre-requisites for upgrade section using **`upgrade feature`** command.

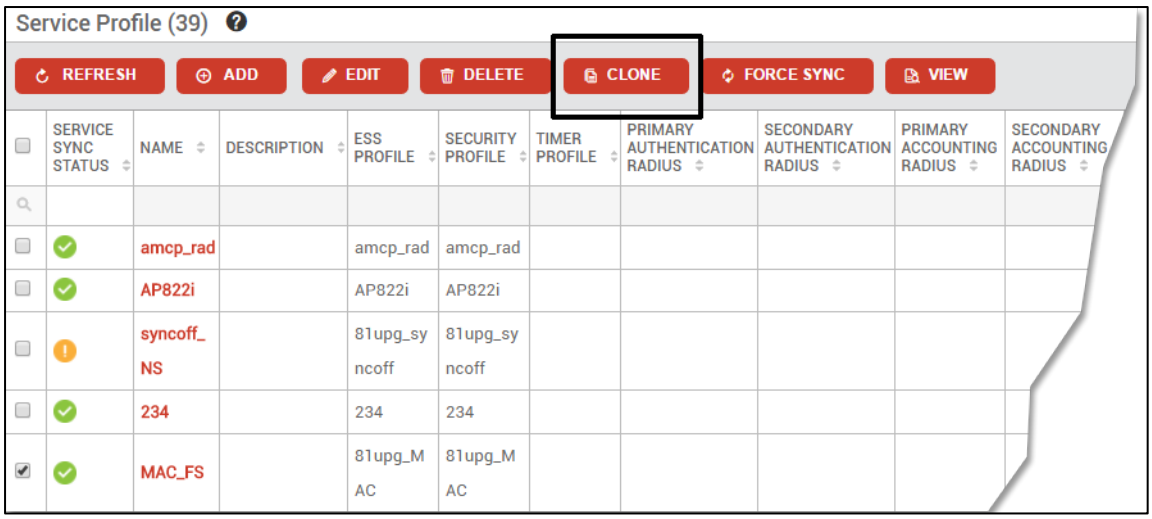
Downgrade

Downgrading FortiWLM to a previous version is not supported. To go back to an older version of FortiWLM, you must do a fresh install of that version on your FortiWLM server.

New Features

Wireless Profile Cloning

You can now clone a wireless service profile instead of creating a duplicate manually. All profiles (except VLAN and GRE) in the service profiles is cloned. For detailed information, see the online help for Service Profile.



Controller Configurations Updated

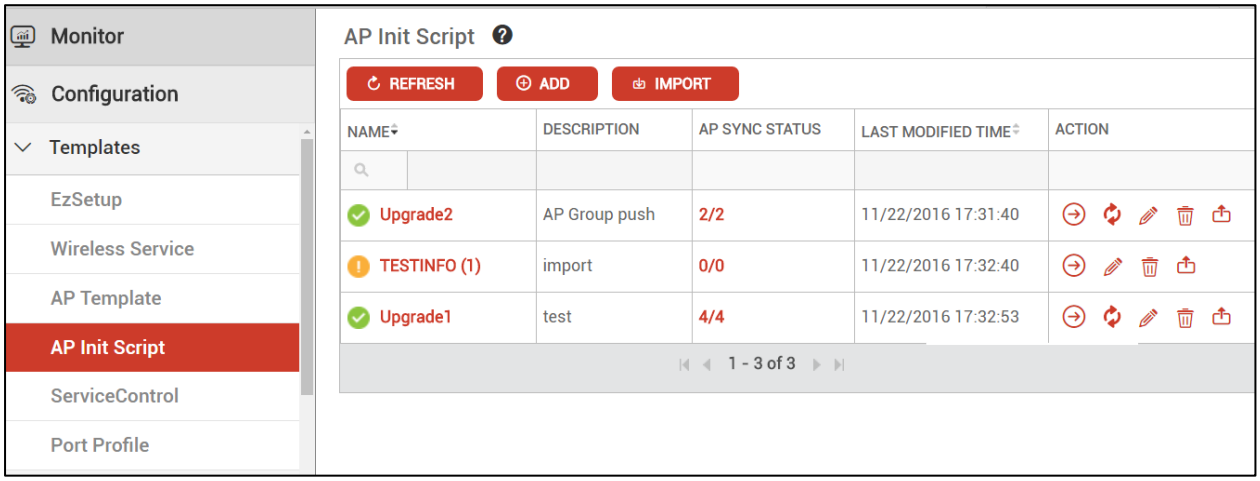
You can now create and push the following controller configurations from FortiWLM. For detailed information regarding each of these features, see the FortiWLC-SD configuration guide:

- AP Init Scipts
- DHCP Profiles
- Guest User Management
- HotSpot 2.0
- MAC Filtering

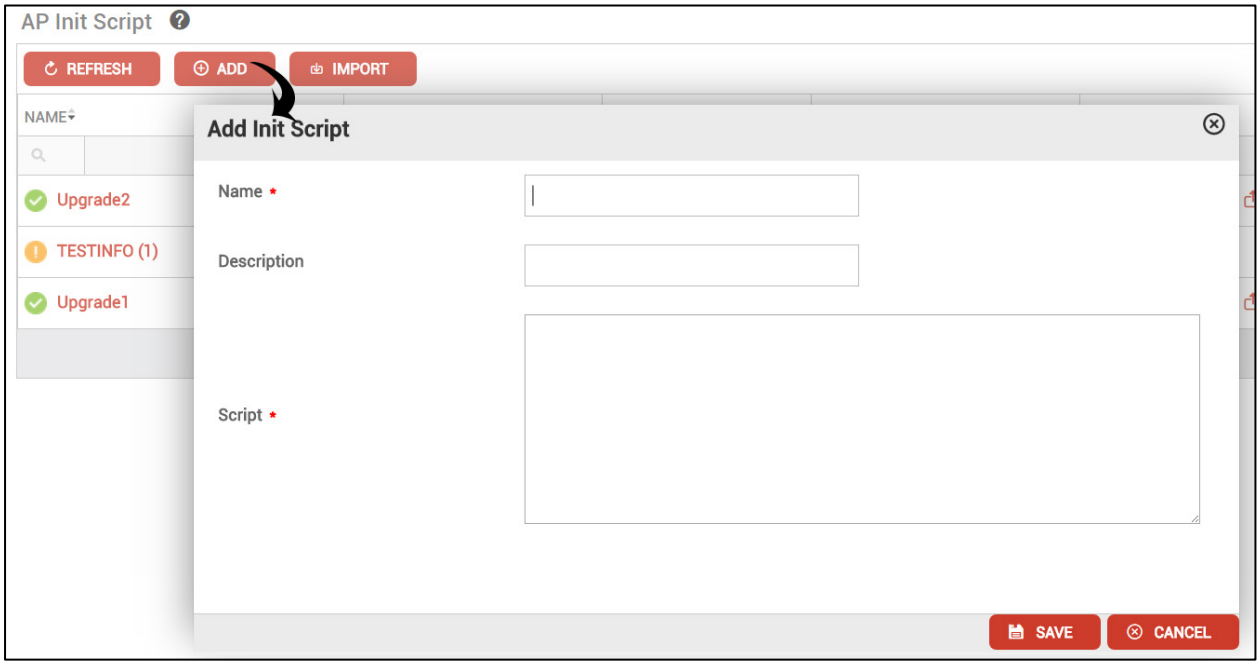
- MESH Profiles
- iBeacon
- QoS Configurations

AP Init Scripts

You can now load AP specific scripts files (for example, AP boot scripts) via FortiWLM and push them to controller APs or AP Groups. The default page shows the list of all scripts and options to push the script to controller APs/AP Groups, edit scripts, import Scripts, and export the script file to be used externally.



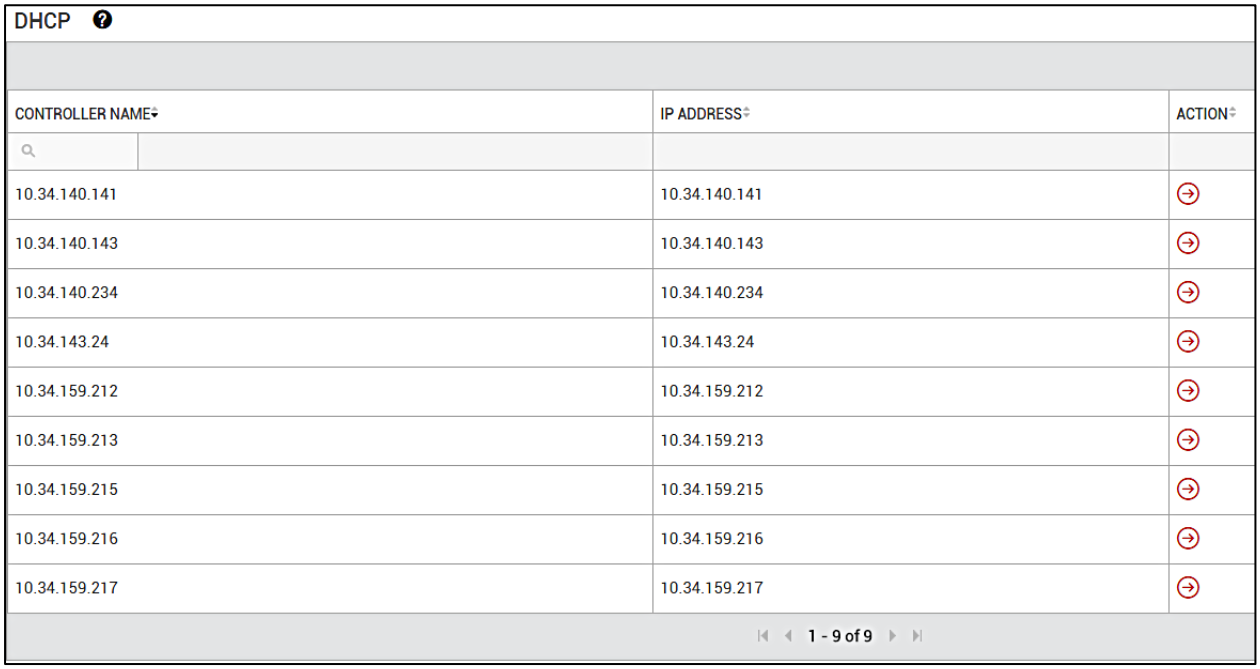
To add a new script, click the ADD button. In the pop-up box, enter a name for the script and provide the script.



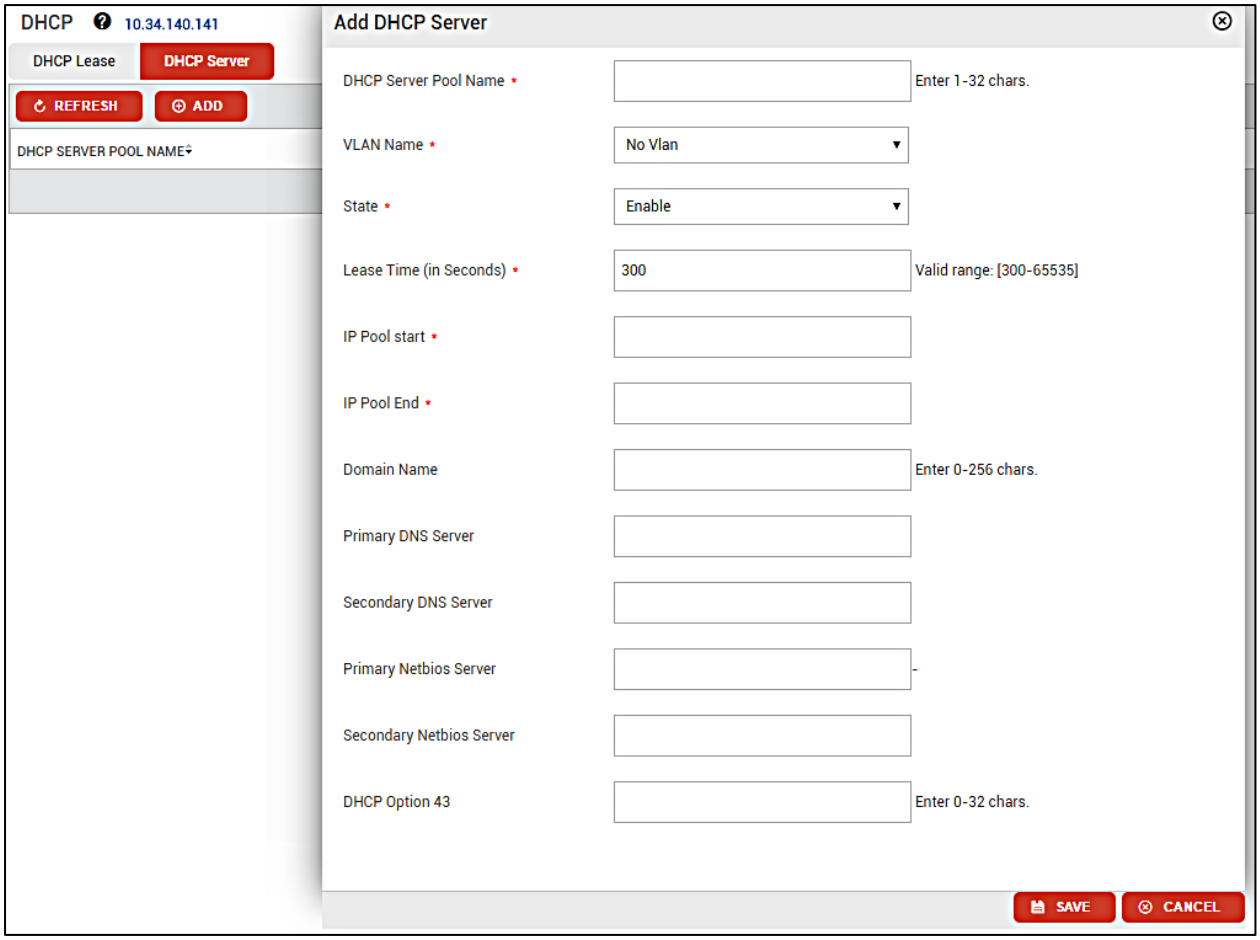
Alternatively, you can load AP Init scripts by importing script files (*.scr), by clicking the IMPORT button.

DHCP Configuration Support

You can now create DHCP configurations from FortiWLM and deploy them to controllers. The default DHCP configuration page lists all online controllers with IP address. To create DHCP configuration for a controller, click the arrow button in the Action column.



In the resultant page, click **DHCP server** and then click the **Add** button.

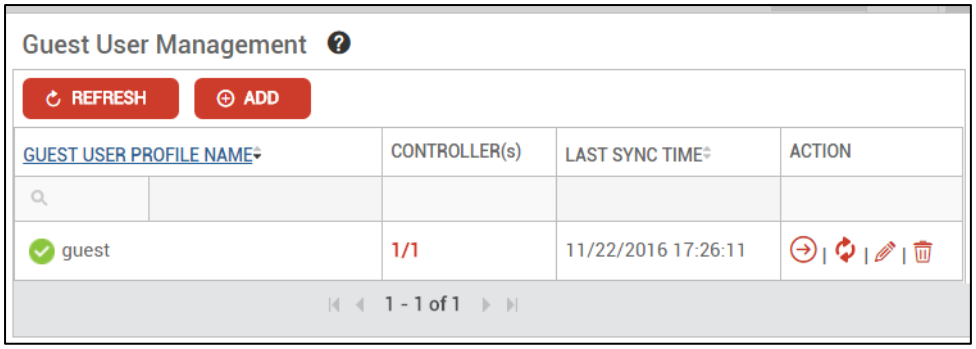


The following table describes the DHCP server information provided. Note that the table will only be displayed after at least one DHCP server entry has been created.

Field Name	Description
DHCP Server Pool Name	The name for the DHCP pool.
VLAN Name	The drop-down list allows you to specify the VLAN to which the DHCP server applies.
Virtual Interface Profile Name	The drop-down list allows you to specify the Virtual Interface Profile to which the DHCP server applies. **Note** This option is only available if the controller is operating in Layer 3 routing mode.
State	Can be set to Enabled or Disabled--this option specifies whether the DHCP server is active.
Lease Time	The duration of the DHCP lease, as configured when the server was created. This value is displayed in seconds.
IP Pool start	The IP address at which the DHCP server will begin assigning addresses.
IP Pool end	The last IP address that can be assigned by the DHCP server.
Domain Name	The Domain name for the DHCP server.
Primary and Secondary DNS Server	The primary DNS server used by the server. A secondary DNS server can also be configured for fallback.
Primary and Secondary Netbios Server	Enter the primary and secondary NetBios server used by the FortiWLM server.
DHCP Option 43	Enter the controller IP address.

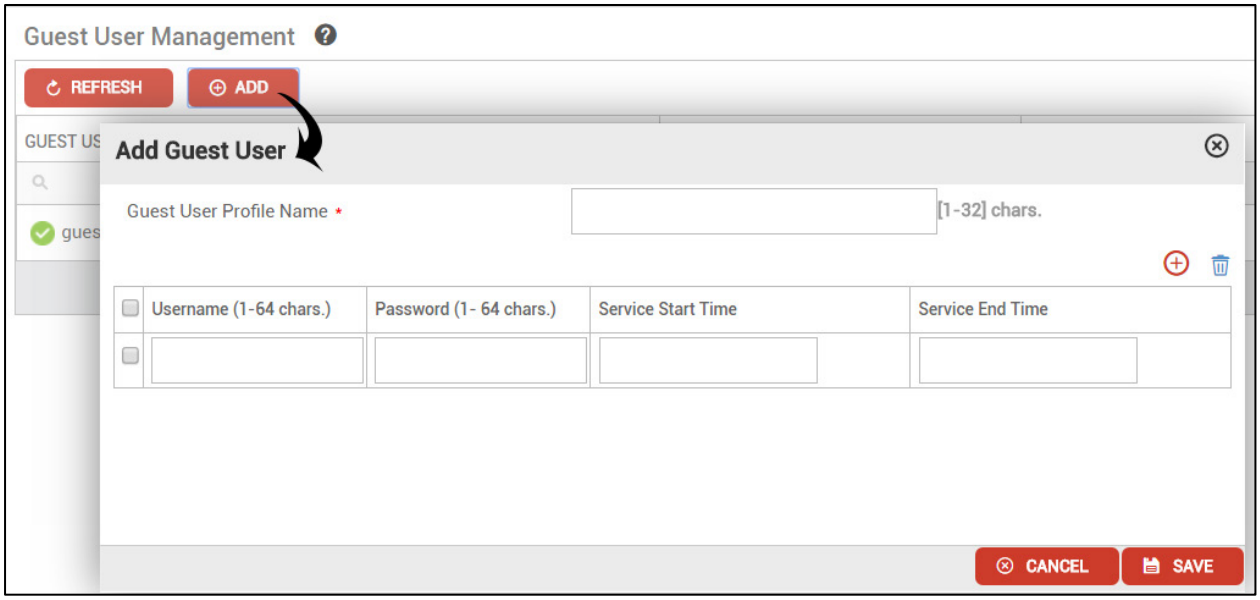
Captive Portal Guest Users

You can now add profiles with a list of guest users that can connect via captive portal based as per the rule defined for the guest user profile.



To create a guest user profile:

Click the **ADD** button



1. Give a name for the guest user profile.
2. Enter a username, password and time limit for this user.
3. Click SAVE to complete the process.
4. Now, assign the guest user profile to a controller.

Select the required guest user profile and click the apply arrow icon to specify the controller IP address.

HOTSPOT 2.0 Support

Supported only on Wave-2 Access Points (FAP-U423EV and FAP-U422EV).

Hotspot 2.0 is a specification by the Wi-Fi Alliance that specifies a framework for seamless roaming between WiFi networks and Cellular networks. The specification is based on the IEEE802.11u standard; a Generic Advertisement Service (GAS) that provides over-the-air transportation for frames of higher layer advertisements between stations APs and external information servers. This feature will allow users to

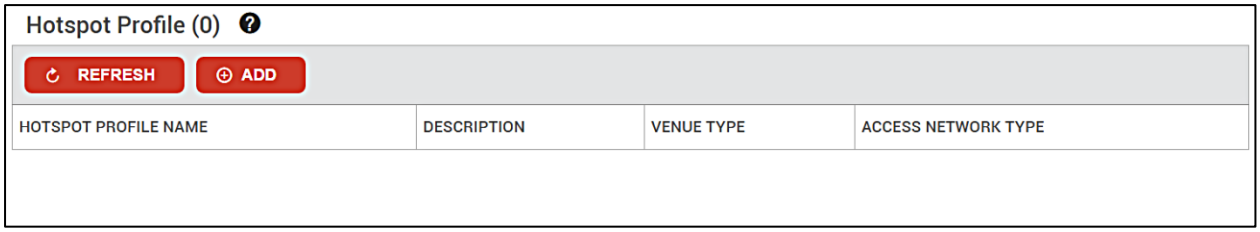
configure hotspot profiles that can (optionally) be connected to existing ESS Profiles as desired. An ESS-profile connected to a hotspot profile will advertise 802.11u capabilities in its beacons.

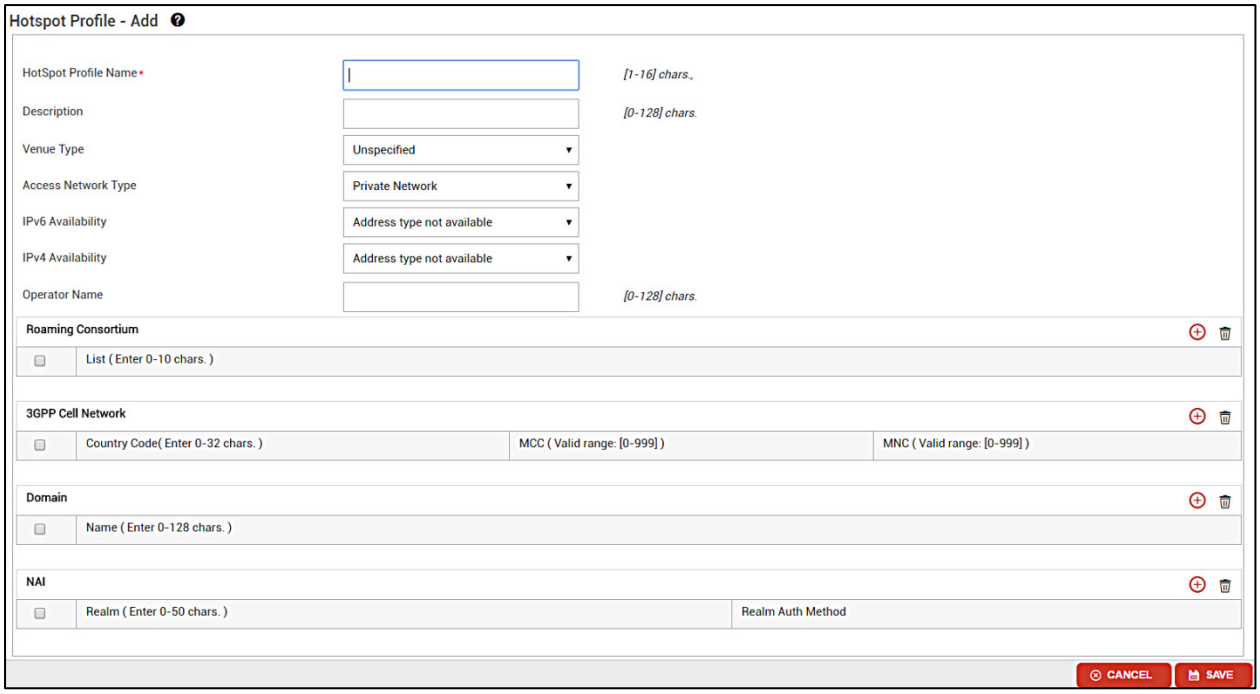
The Hotspot Profiles can be created from the Configuration > Profiles > Hotspot page. By default, the page shows the following details about a HotSpot Profile.

Field	Description
Hotspot Profile Name	The name of the Hotspot profile
Description	Description about the Hotspot profile
Venue Type	The venue type field in the information element provides additional information about the group and type of hotspot venue. The hotspot operator shall configure the Passpoint AP with one of the venue group description values, such as "business" or "educational" from the drop down box.
Access Network Type	The access network type field is automatically included in the IEEE 802.11u interworking element present in beacon and probe response frames in PAPs. Mobile devices can use this information when selecting a hotspot. The access network types are as follows: • Private Network • Private Network with Guess Access • Chargeable Public Network • Free Public Network • Personal Device Network • Emergency Services Only Network • Test or Experimental Network • Wildcard Network

Add Hotspot Profile

To add the Hotspot profile, click the ADD button:





Enter the following details:

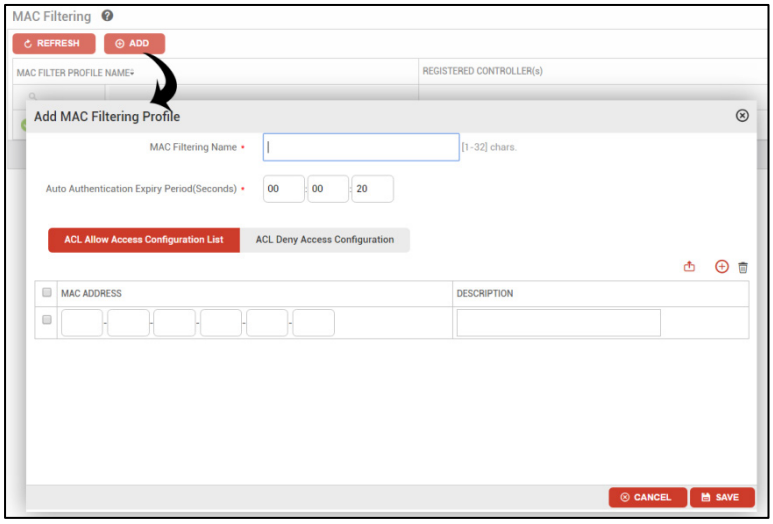
Field	Description
Hotspot Profile Name	Enter Hotspot profile name; this is a required field and the valid range 1-16 characters.
Description	Enter the description provided for the Hotspot profile
Venue Type	Select the venue type from the drop-down list. The venue type field in the information element provides additional information about the group and type of hotspot venue. The hotspot operator shall configure the Passpoint AP with one of the venue group description values, such as "business" or "educational" from the drop down box. The default selection is displayed as Unspecified.
Access Network Type	Select the Access Network type from the drop down list. The access network type field is automatically included in the IEEE 802.11u interworking element present in beacon and probe response frames in PAPs. Mobile devices can use this information when selecting a hotspot. The default selection is displayed as Private Network, and the options are as follows: • Private Network • Private Network with Guess Access • Chargeable Public Network • Free Public Network • Personal Device Network • Emergency Services Only Network • Test or Experimental Network • Wildcard Network
IPv6 Availability	Select the IPv6 availability from the drop-down list. The default selection is Address type not available, and the options are as follows: • Address type available • Address type not available • Availability of the Address type not known

Field	Description
IPv4 Availability	Select the IPv4 availability from the drop-down list. The default selection is Address type not available, and the options are as follows: • Address type available • Address type not available • Availability of the Address type not known • Port-restricted IPv4 address available • Single NATed private IPv4 address available • Double NATed private IPv4 address available • Port-restricted IPv4 address and single NATed IPv4 address available • Port-restricted IPv4 address and double NATed IPv4 address available
Operator Name	Enter the operator name for the Hotspot profile. The valid range is 0-128 characters.
Roaming Consortium	Enter the roaming ORG ID for the Hotspot profile. The valid range is 0-64 characters.
3GPP Cell Network	• Enter Country Code. • Enter the 3GPP cell network MCC; the default value displayed is 0, and the valid range is 0-999. • Enter the 3GPP cell network MNC; the default value displayed is 0, and the valid range is 0-999.
Domain Name	Enter the domain name for the Hotspot profile. The valid range is 0-128 characters.
NAI	NIA Realm: Enter the NAI realm. Realms that can authenticate a mobile device's username/password or certificate credential shall be added to this list. The valid range is 0-50 characters. Realm Auth Method: Select the NAI realm authentication method from the drop-down list. The default selection is EAP TLS Certificate and the options are as follows: • EAP TLS Certificate • EAP TLS MSCHAPv2 Username/Password • EAP SIM • EAP AKA • EAP AKA`

MAC Filtering Support

You can now create MAC filtering rules from FortiWLM and deploy them to controllers.

Click the ADD button, to add a MAC filtering rule,



In the Add MAC Filtering Profile window, enter the following:

1. Give a name to identify the filter profile.
2. Specify the time until which this rule is enforced.
3. You can create a rule to allow access or deny access. Click the appropriate button (ACL Allow Access Configuration List or ACL Deny Access Configuration List) before entering the MAC address.
4. You can manually enter the MAC address of clients or click the Import button to get a list of MAC address from a text file. Enter MAC addresses one per line.
5. Click Save to complete this step.

Mesh Configuration Support

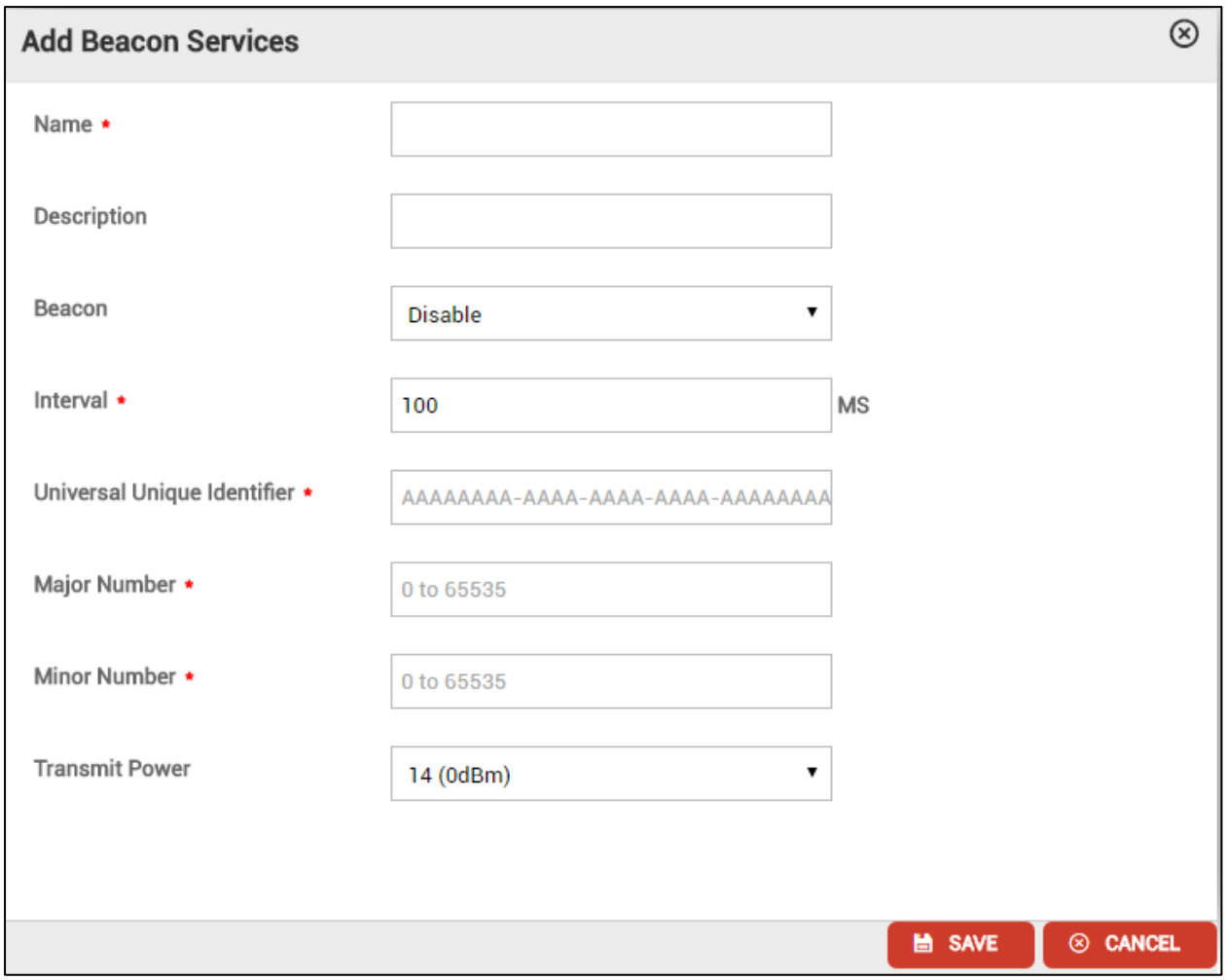
You can now create mesh configurations from FortiWLM and deploy them to controllers. The default page lists all online controllers.

iBeacon Services

With this release, 11ac APs can now send iBeacons that will help advertise hyperlocal content to users in context to their location.

Supported APs: AP122, AP822, AP832 (the APs will require a Bluetooth dongle)

To use the beacon services, navigate to Configuration > Controller Configuration > iBeacon and click the **Add** button to enter the following details:

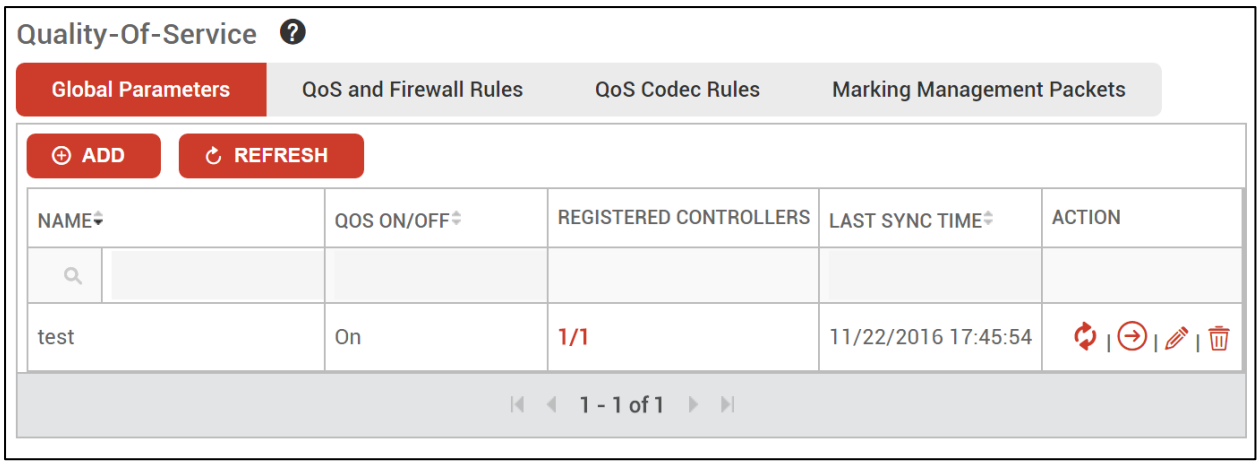


- Enter a **name** for the beacon service and provide a **description**.
- Enable **Beacon** to start the services
- Select the time **interval** at which the beacons are sent.
- Enter a **Universal Unique Identified** (UUID) that is specific to your network and also specify the respective **Major Number** and **Minor Number**.
- Select **Transmit Power.**

After creating a profile, click the action arrow to push this to a controller.

QoS Rules

You can now configure QoS rules and push them to controllers.



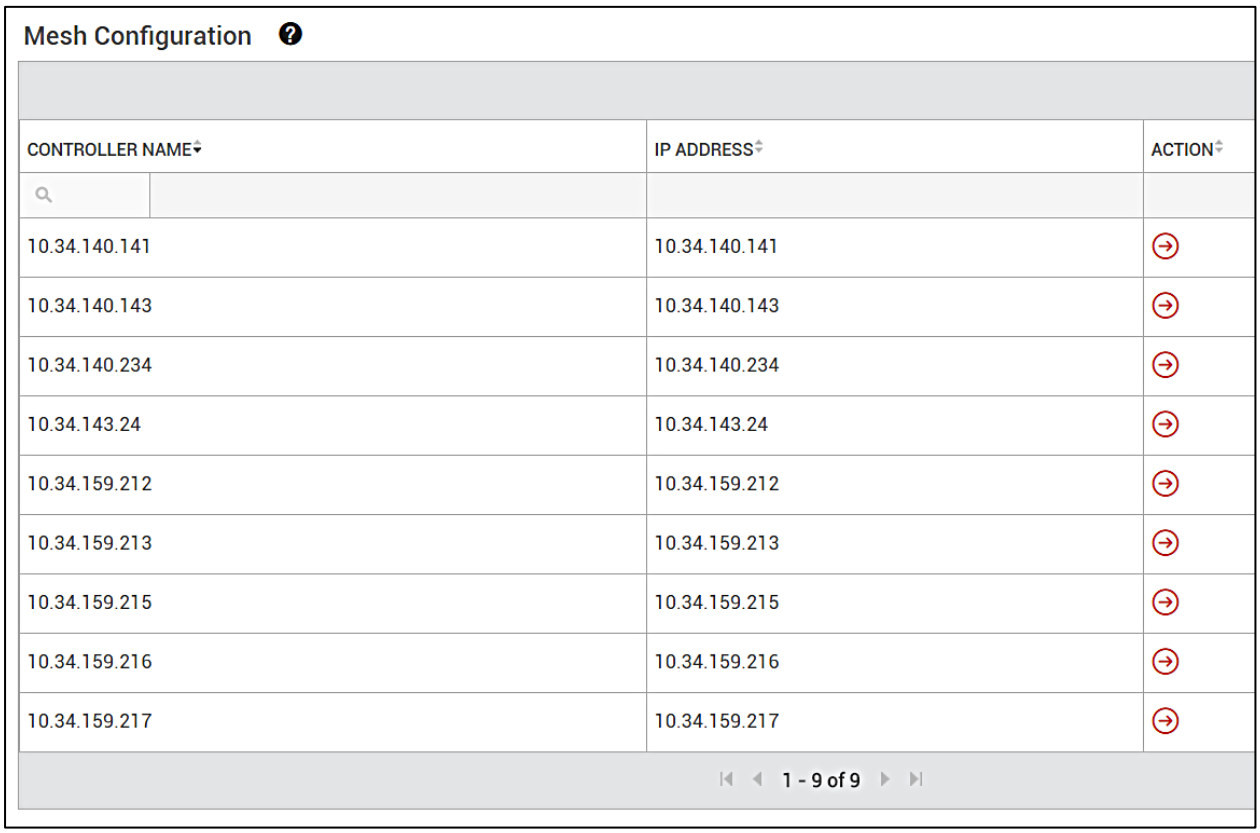
The QoS section allows you to configure the following:

Global Parameters and Marking Management Packets

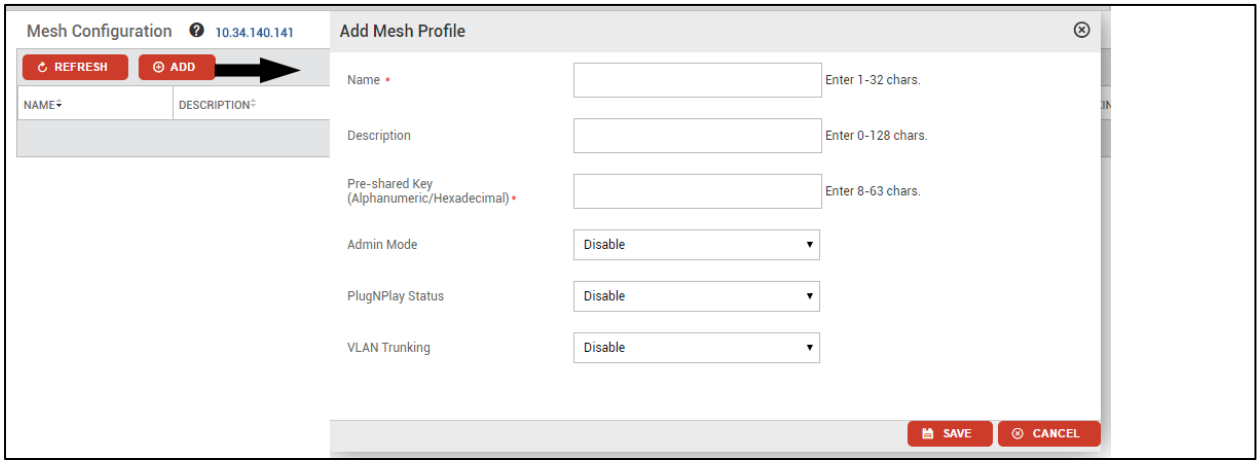
Value configured as global parameters and for Marking Management Packets will take precedence over values configured from FortiWLC-SD. When pushed to the controller, these values will override the controller values and will be replaced with the parameters configured from FortiWLM.

QoS and Firewall Rules & QoS Codec Rules

These rules start with ID 6000 to differentiate them from FortiWLC-SD rules. In FortiWLM you can combine multiple rules into a profile and push them to controllers.



To create a mesh configuration on a controller, click the arrow button in the Action column.

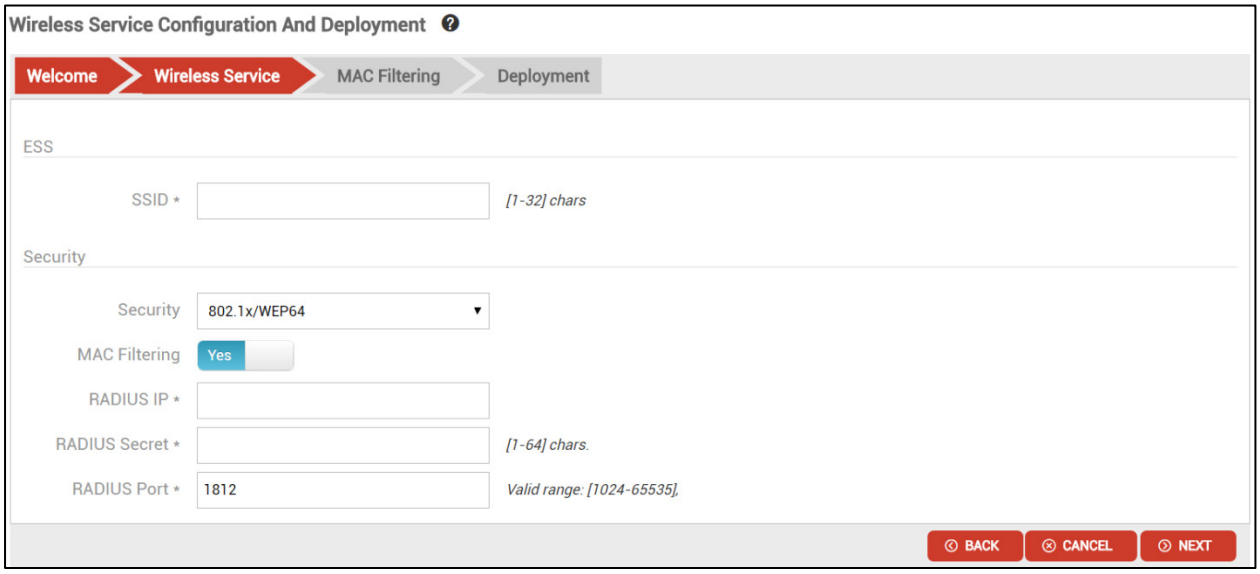


In the resultant page, click the Add button to create the Mesh configuration. The following table (Configuration > Wireless > Mesh) describes the current mesh configuration. Note that the table will only be displayed after at least one Mesh network has been created.

Name	The name provided for the mesh.
Description	A description for the mesh (e.g., the mesh's location or service region).
Admin Mode	Indicates whether Admin Mode is enabled or disabled.
PlugNPlay Status	Indicates whether PlugNPlay is enabled or disabled for the mesh.

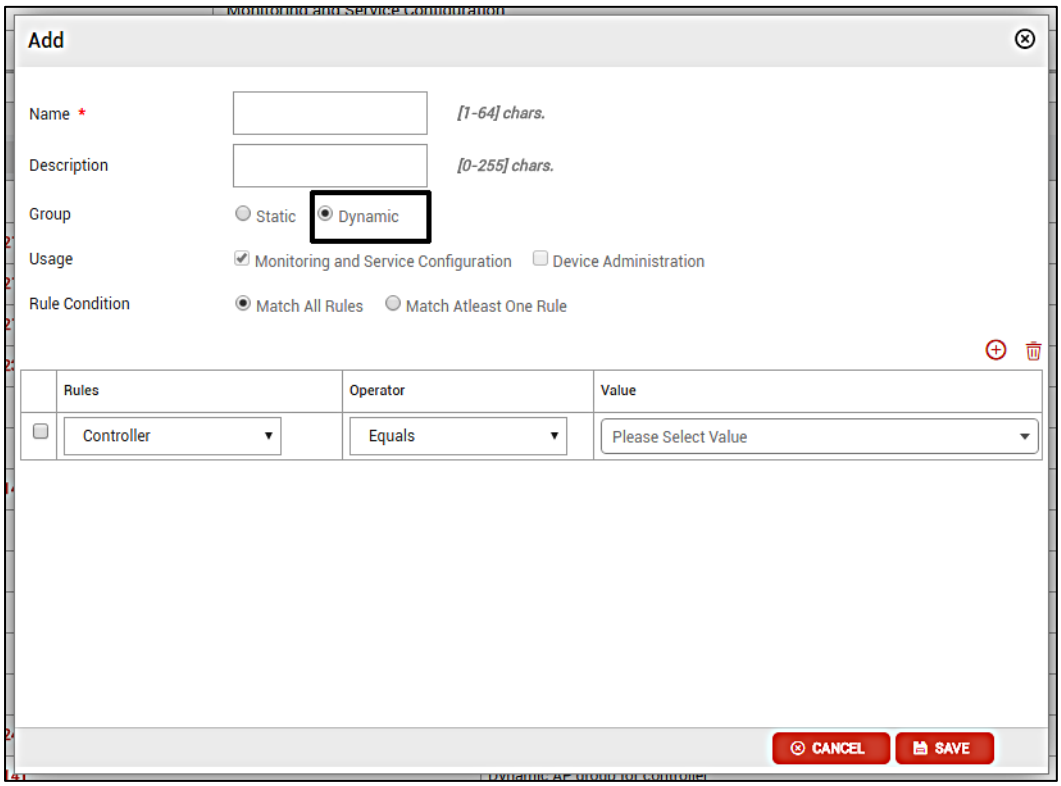
Simplified Configuration Wizard

The Ez Setup is a step by step wizard to easily create wireless configurations with any security options and deploy them to your controllers and AP groups. Additionally, you can add MAC filtering options to your wireless configurations.



Dynamic AP group

Dynamic grouping allows you create AP groups based on various rules. By default, APs connected to a controller that is added to an AP group based on the controller's IP address. This is also called the default dynamic AP group.



Rules can be created using the following conditions:

- Controller IP address
- Location name
- Building name
- Floor number
- Discovery Type
- AP Model
- Software Version
- Parent MAC Address
- Indoor or Outdoor APs

NOTE:

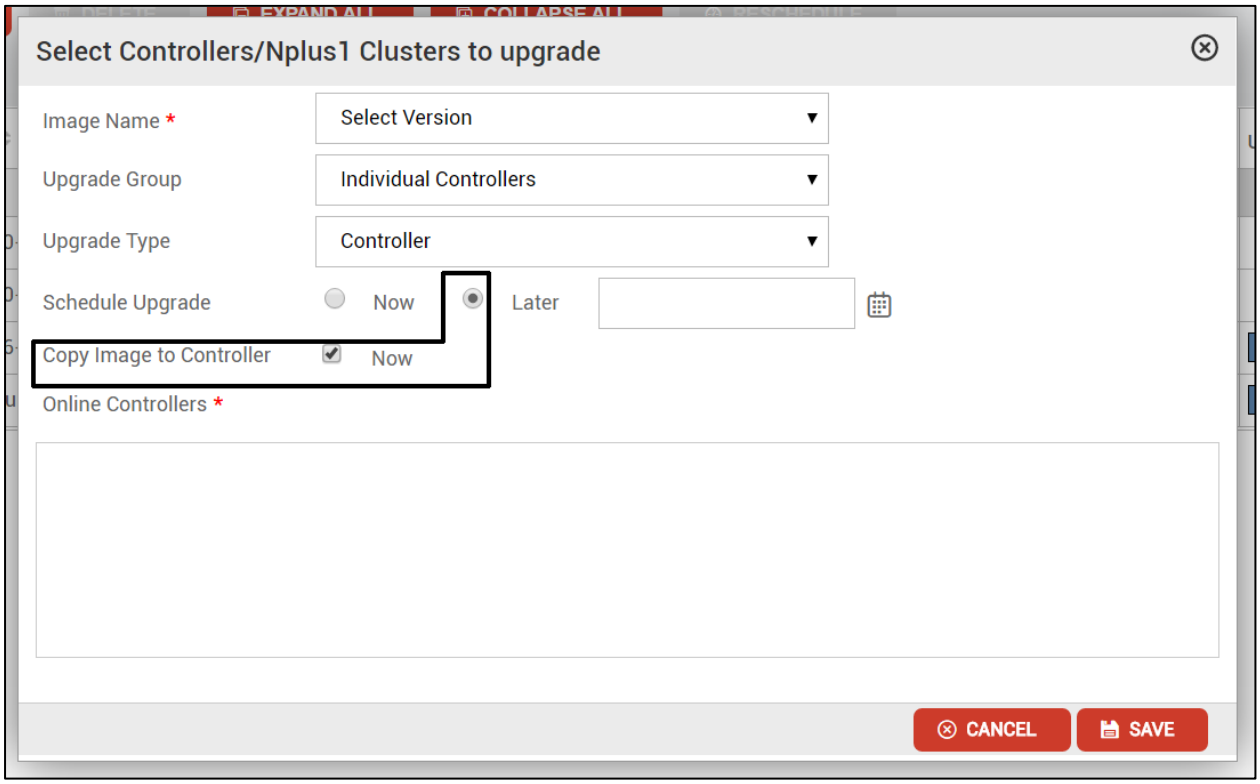
1. The default group cannot be modified or deleted, and APs in that group cannot be removed. Dynamic groups are available only for service and monitoring and cannot be used for device administration
2. An AP can exist in more than one dynamic groups.
3. A dynamic group can be created inside a static group.
4. Any modification to the rule will affect the APs in the group.

Validate PCI Compliance

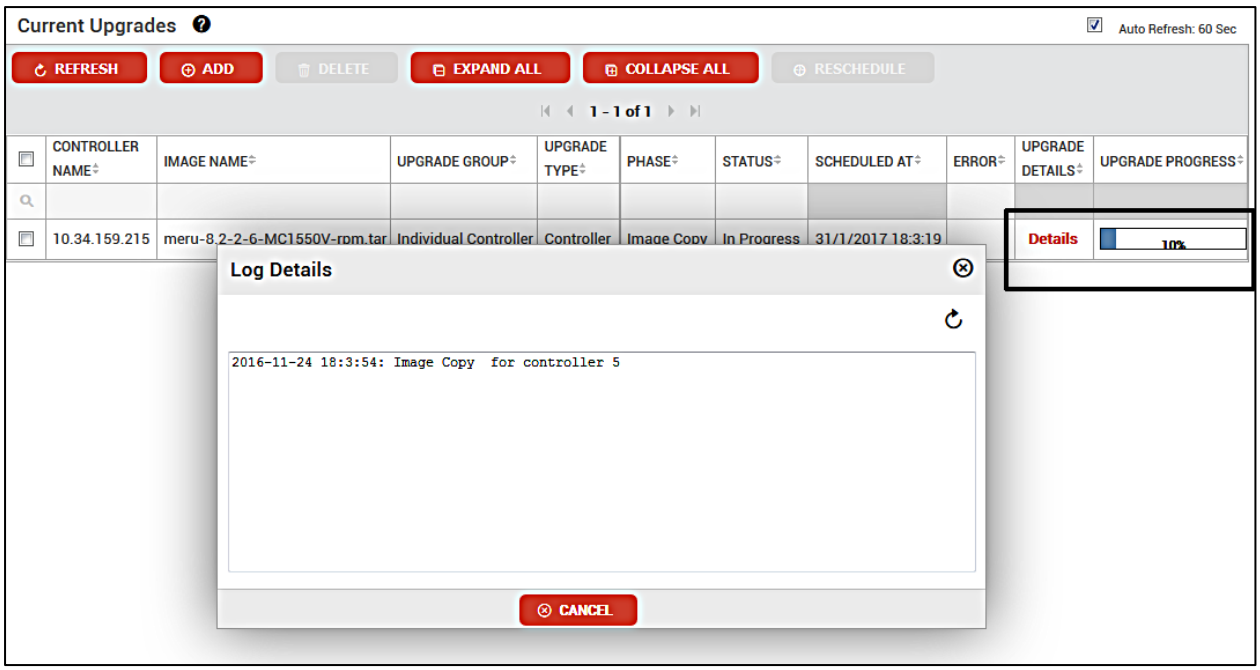
FortiWLM can be validated against specific PCI requirement compliances as listed at the Reports&Notify > Reports > PCI page.

Enhancements to Upgrade Management

You can now copy the controller image into the server and initiate installation process later as per a scheduled time.

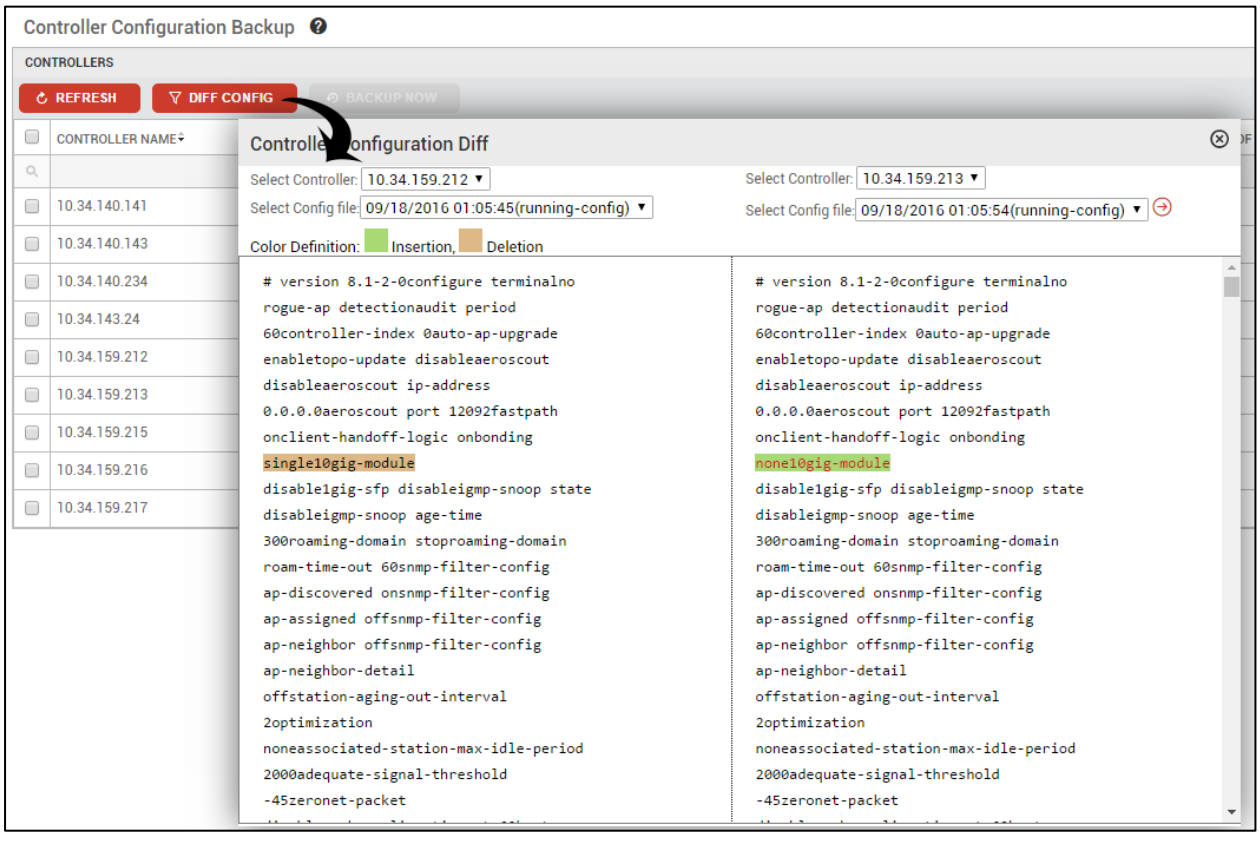


After you click the **Save** button, the page is refreshed to show the progress of image copy. Click the Details link to see detailed progress.



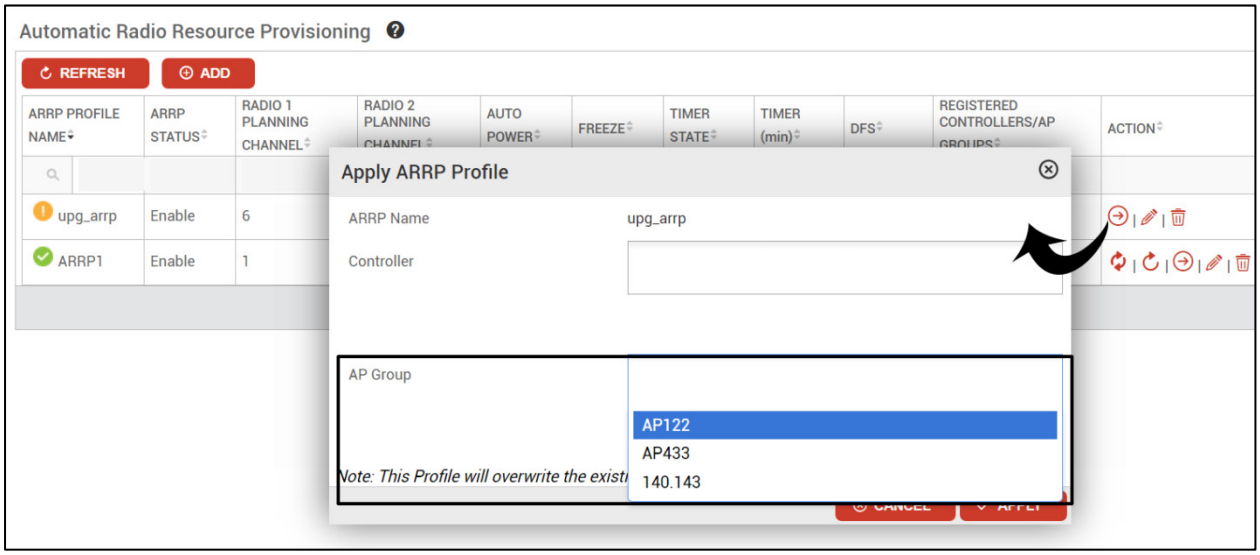
Backup controller configuration

You can view differences between startup and running configuration of the same controller or two difference controllers and apply running-config to startup-config or startup-config to running-config.



Apply ARRP Profiles to AP Groups

You can now apply ARRP profiles to static AP groups.

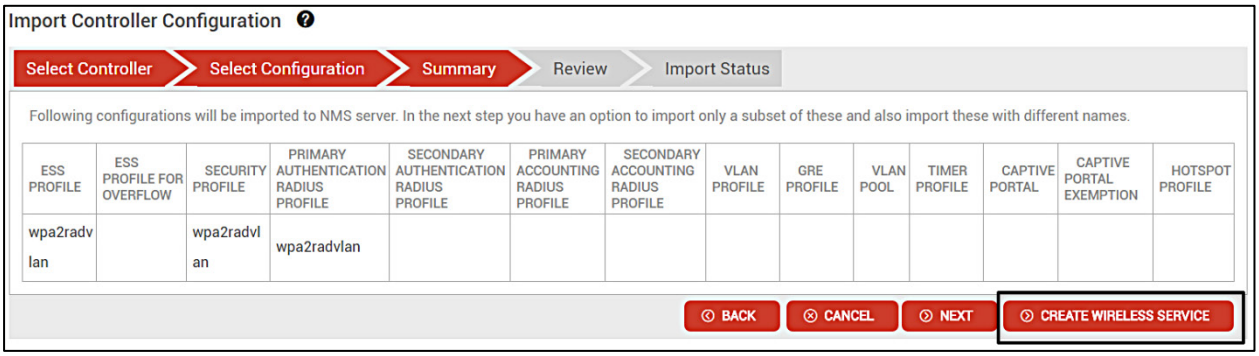


Configuration Migration

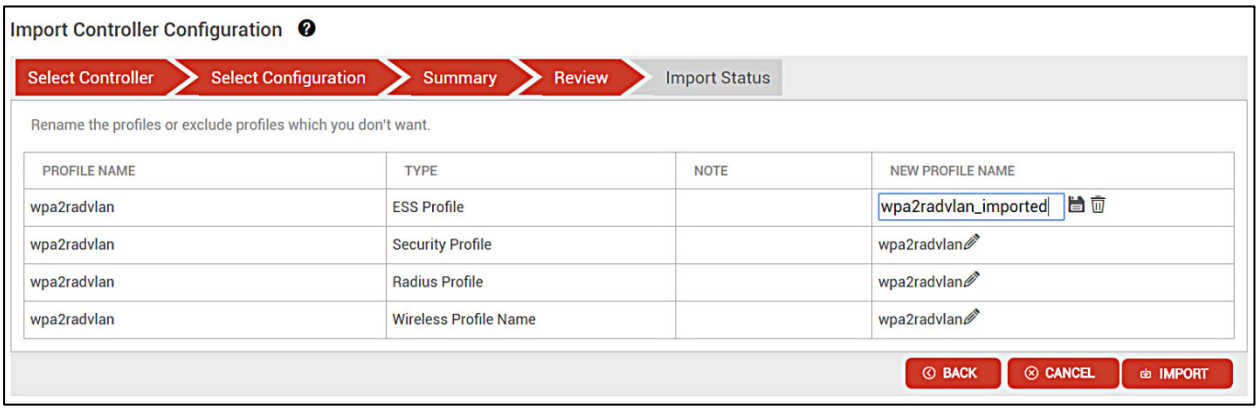
You can now easily create a wireless service profile based on the imported configurations (ESS, Security) from another controller.

To create a new wireless service profile from configuration imported from another controller:

1. Navigate to Configuration > Controller Configuration > Import
2. Select a Controller and click Next to import all configurations from that controller.
3. Click an ESS profile from *Available ESS Profile* list and click right (>>) arrows to select.
4. In the Summary tab, click the Create Wireless Service button to create a new wireless service profile.



5. In the Review tab, the new profile names are listed. You can rename them (if required) to differentiate them from regular profiles.

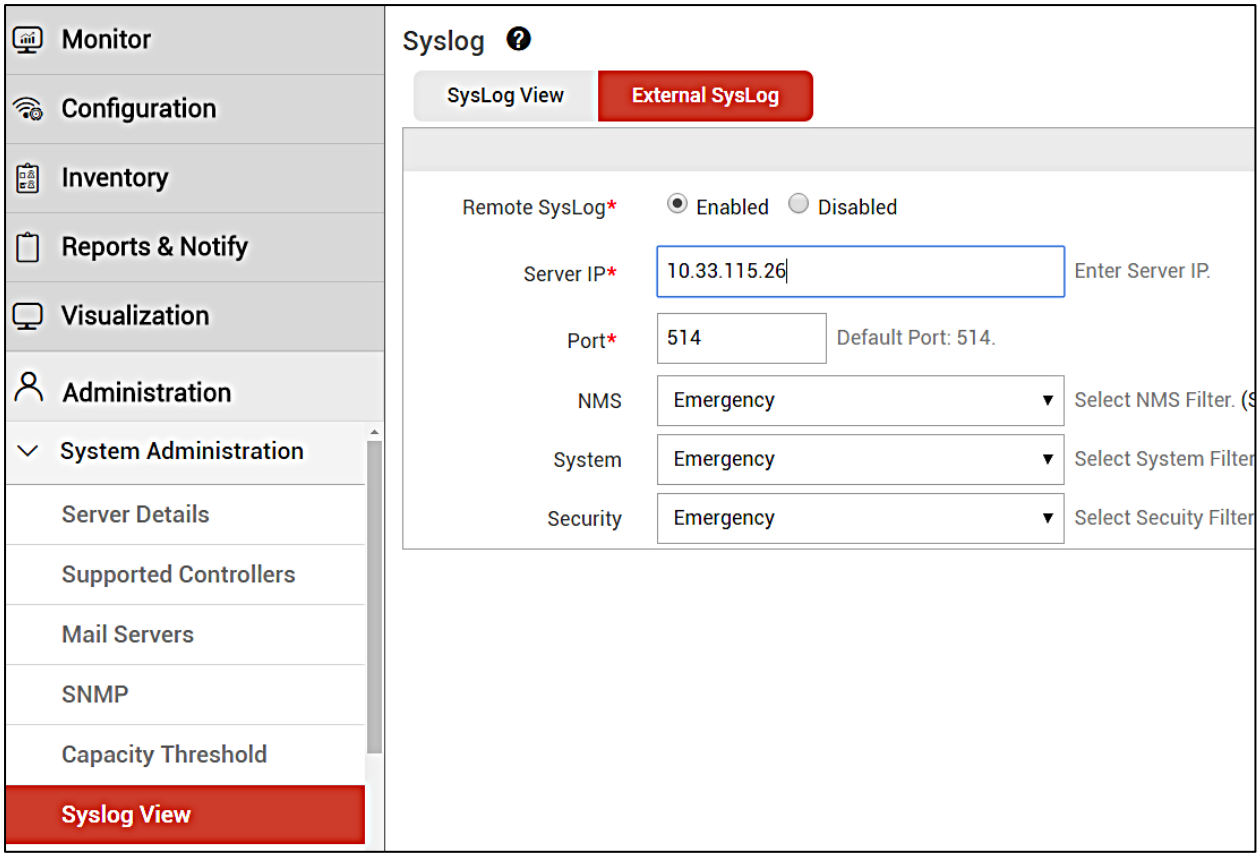


6. Finally, click Import to import that profile. The imported profiles are listed in the Configuration > Templates > Wireless Service page.

Export Syslog to External Server

Syslog from a FortiWLM device can be exported to an external syslog server. To export to an external server, configure the server details the type of logs to be exported.

Navigate to Administration > System Administration > Syslog View and select the External Syslog tab.



Enter the following details

- Select **Enable** to allow exporting the syslogs to an external syslog server.
- Server IP: The IP address of the external syslog server
- Port: The port at which the external syslog server will accept incoming connection from FortiWLM
- NMS, System, and Security : Select the type of logs from each of the category that will be sent to the external syslog server.

Factory Reset

You can now reset your FortiWLM device to its last known default configuration settings. All other configurations and settings are erased.

- Proceed with extreme caution. We recommend that you take a backup of any data before doing a factory reset. Factory reset will erase all data from your device.

Before Performing Reset:

- Ensure that you have console access to your device.
- Disable HA

Configurations that are pushed to controllers, APs and AP Groups are not affected.

Factory reset can be performed only from the command line interface of your FortiWLM device. Login to the command line interface and run the **`reload default factory`** command.

User Interface Enhancements

Session Timeout

As part of PCI compliance, unattended FortiWLM login session will timeout in 5 minutes. The timeout duration is configurable with Never, 5, 15, 30, and 60 minutes. Select ***NEVER***, to prevent a session being timed out.

This option is available in **Administration** > **System Administration** > **Maintenance** > ***USER INTERFACE PREFERENCE*** section

By default, the timeout is set at 5 minutes.

Password Rules

By default, FortiWLM requires users to follow strict password rules as defined in the PCI compliance section. However, you can now allow users to create simple passwords by disabling this condition.

This option is available in **Administration** > **System Administration** > **Maintenance** > ***USER INTERFACE PREFERENCE*** section.

API Support

FortiWLM exposes the following set of REST APIs that allows you to query the FortiWLM server to get and post the following sub-system information.

- AP Groups
- Syslog / Activities
- Station
- Access Points
- Network Summary
- Alarms
- Controllers
- ESS
- Security
- Wireless

For example, to get list of APs, send the following *get* request with input parameters:

Request: `https://<FortiWLM-Server-IP>:5000/api/v1.0/apgroupinventory`

Response

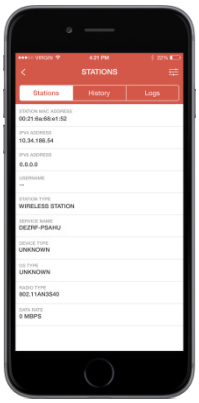
```
{
  “items”:[

  {
    “apGroupType”:1,
    “apGroupID”:2,
    “apGroupName”:”sample”
  }
```

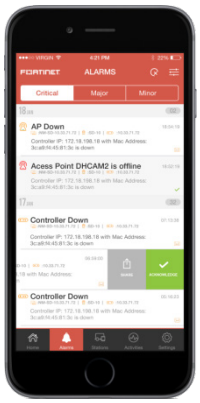
iOS APP for FortiWLM Monitoring

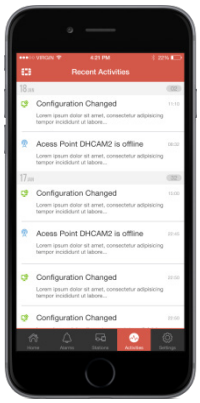
The FortiWLM monitoring component is now available as an iOS APP. Users can install this in an iPhone to monitor and view the following:

- Network Dashboard
- Search and view station details
- Alarms
- Recent activity list

Network Dashboard	Station Information	Alarms	Recent Activities







The FortiWLM monitoring APP is available for beta testing. If you are interested in testing this app, please contact Fortinet Support.

Fixed Issues

Bug ID	Description
0389541	Fixed issues that caused the *mailboxes Critical 'EzRF Agent' (mbxId 100)* message.
0386003	Fixed incorrect *Service Usage Trend Report for Enterprise*.
0405972	Fixed license error issues on SAM running on WLM
0405957	HA is not supported on FortiWLM 100D and SA250.
0400955	Channel 64 is added as a valid channel in Wireless IPS.
0369991	Fixed incorrect statistics for controllers on network manager.
0399624	Fixed issues that caused WebUI page load delays.
0399625	Fixed checksum issues when upgrading from 8.1/8.2 to 8.3
0399618	Fixed WebUI display issues in 1200x800 screen resolution.
0385861	Notification filter is updated with the following alarms: • AP CPU Usage High • AP Runtime error • AP Software Version Mismatch • Alarm History full • Controller CPU Usage High • Controller Memory Usage High • Event Log Full • Watchdog Failure

Bug ID	Description
0391629	Fixed service control chart issues to display station counts correctly.
0378747	Fixed incorrect status issue related to controller management.

Known Issues and Limitations

Bug ID	Description
0396392	Users can create a dynamic group with the same name that is already used by the system.
0401431	Unable to create Captive Portal Exemption in IE Browser.
Limitations	
0414400	MIMO mode in Radio profile is not supported.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service